IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
Harrisonburg Division

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH **FELICIAJACKSON0247@GMAIL.COM** THAT IS STORED AT PREMISES CONTROLLED BY **GOOGLE, LLC.**	Case No. 5:20-mj-00040

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Brian McCarthy, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Google, LLC ("Google"), an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the United States Department of Agriculture, Office of Inspector General ("USDA/OIG"), and have been since 2019. I am currently assigned to the USDA/OIG Office in Richmond, VA. I am authorized to conduct criminal investigations on behalf of USDA/OIG. Prior to my employment with USDA/OIG, I was employed as a U. S. Postal

Inspector with the U. S. Postal Inspection Service for sixteen years. Prior to my employment as a U. S. Postal Inspector, I was employed as a Special Agent with the Virginia Department of Alcoholic Beverage Control for approximately seven years. I have participated in the execution of subpoenas, search warrants, and arrest warrants, and have investigated various federal violations, including offenses pertaining to fraud and financial crimes. My duties include, but are not limited to, investigations pertaining to Title 18 of the United States Code.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The information contained in this affidavit comes from my training and experience, my review of records, my direct observations, and through information obtained from other law enforcement officers.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 U.S.C. § 1343 have been committed by the user of feliciajackson0247@gmail.com. There is probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States…that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. Romance scammers lure people with phony online profiles, often lifting photos from the Internet to create attractive and convincing personas. They might make up names or assume the identities of real people. Reports indicate that scammers are active on dating apps, and also on social media sites that aren't generally used for dating.

7. Once these fraudsters have people by the heartstrings, they say they need money, often for a medical emergency or some other misfortune. They sometimes claim to be in the military and stationed abroad, which explains why they can't meet in person. Pretending to need help with travel costs for a long-awaited visit is another common ruse.

8. According to the Federal Trade Commission, romance scams rank number one in total reported losses, with more losses attributable to romance scams than to any other type of consumer fraud identified in the Consumer Sentinel database. The FTC reports that in 2018, Consumer Sentinel had more than 21,000 reports about romance scams, and people reported losing a total of $143 million, which is more than any other consumer fraud type identified in Sentinel.[1]

9. According to the FTC, the median individual loss to a romance scam reported in 2018 was $2,600.00, about seven times higher than the median loss across all other fraud types. People often reported sending money repeatedly for one supposed crisis after another.

At all times relevant to this matter, David WHITACRE resided in Winchester, Virginia, which is within the Western District of Virginia. WHITACRE was a participant in a USDA funded program through the Farm Service Administration (FSA). Specifically, On July 15, 2014, Whitacre applied

[1] https://www.ftc.gov/news-events/blogs/data-spotlight/2019/02/romance-scams-rank-number-one-total-reported-losses

for and received a Farm Operating Loan from USDA/FSA in the amount of $259,000.00. The loan was assigned Loan Number 44-01-OL and was for the purpose of purchasing cattle and re-financing existing debt. This loan was "re-scheduled" twice, once on December 6, 2017, and again on February 13, 2019.

10. On February 13, 2019, Whitacre re-scheduled the existing loan into a new loan with Loan No. 44-03-OL and in the amount of $226,669.18. Whitacre signed and executed FSA Form FSA-2028, *Security Agreement*, in conjunction with this new loan. In the Security Agreement, Whitacre pledged 179 head of cattle as collateral securing the new loan.

11. On various dates, beginning on July 8, 2019, and continuing through November 18, 2019, Whitacre sold cattle that were pledged as collateral to the USDA/FSA, without permission from USDA/FSA, as required by the loan documents. According to Farmer's Livestock Exchange, Inc. records, Whitacre sold a total of 128 head of cattle, generating $70,880.35 in net proceeds during this time period. The last check, dated November 18, 2019, was intercepted by USDA/FSA and was applied towards the loan. The remaining $53,969.66 was not paid to USDA/FSA.

12. On October 9, 2019, Whitacre attended an in-person meeting with USDA/FSA Farm Loan Officer Robert Swanson. During this meeting, Whitacre informed Farm Loan Officer Swanson that "he had met a lady online who wanted to marry him and he honestly believes she is going to get about $500k in December to pay in full his FSA debts." Farm Loan Officer Swanson indicated that he "cautioned him fervently about this arrangement" and "told him not to send any party any money." Farm Loan Officer Swanson also provided Whitacre a copy of FSA Form FSA-2571, *Agreement for Voluntary Liquidation of Chattel Security*, and discussed the

penalties involved with collateral conversion and also discussed with Whitacre the advantages of a voluntary sale of his farm versus a foreclosure.

13. On November 14, 2019, USDA/FSA Farm Loan Officer Robert Swanson mailed a letter, via both regular U. S. Mail as well as Certified Mail, to Whitacre at his address of record in Winchester, VA. The letter requested an in-person meeting on November 20, 2019, and included FSA Form 4-FLP, Exhibit 31, *Notification of Unauthorized Use of Proceeds*.

14. On November 20, 2019, Whitacre attended this in-person meeting with USDA/FSA Farm Loan Officer Swanson. During this meeting, Farm Loan Officer Swanson reviewed FSA Form 4-FLP, Exhibit 31, *Notification of Unauthorized Use of Proceeds*, with Whitacre, discussed the serious nature of collateral conversion, and demanded payment for or replacement of the disposed collateral within thirty days. Swanson indicated that he, again, informed Whitacre that he "was pretty certain that he was being scammed." Swanson also requested written proof of the California contacts.

15. On December 11, 2019, Whitacre attended another in-person meeting with Farm Loan Officer Swanson at the Strasburg USDA/FSA Office. In this meeting, Whitacre provided the following documents to Farm Loan Officer Swanson:

A.) A purported "Power of Attorney and Affidavit for Change of Ownership" from a court in Ottawa, Canada regarding "5 BARS OF PURE ALLUVIAL GOLD BARS WEIGHING 62 KG."

B.) A copy of an email from "Felicia Jackson" at feliciajackson0247@gmail.com, sent to Whitacre and dated November 27, 2019. The email states in part that she "got knocked down by a vehicle and was admitted at the hospital yesterday." The email

goes on to state that "it's a bad news," and that she "can't walk" and is in need of "immediate surgery."

C.) Photograph of a female in a hospital bed with a bloody and bandaged arm.

D.) Swanson accepted these documents from Whitacre, but told him that he believed that Whitacre was "being taken advantage of." USDA/FSA personnel then referred this matter to the USDA/OIG.

16. On January 16, 2020, USDA/OIG Special Agents interviewed WHITACRE at his residence. WHITACRE admitted to selling cattle that were pledged as collateral to USDA/FSA and provided a written statement. WHITACRE advised that he met a female on the internet in approximately July 2019 and that this female was in the process of sending him gold bars. WHITACRE advised that he had been selling his cattle in order to send money to this female for the purpose of moving the gold bars across the country. WHITACRE advised that he had sent money to "Felicia Jackson" in California via both wire transfer and U. S. Mail. WHITACRE estimated that he had sent approximately $35,000.00 to "Felicia Jackson." WHITACRE also advised that he had sent "Felicia Jackson" $1,200.00 for a plane ticket (date uncertain). USDA/OIG Special Agents notified Whitacre during this interview that they believe the "Felicia Jackson" and gold bar story to be a fraud, and that agent's do not believe that Whitacre will receive any gold bars. Agents also informed Whitacre that he was not permitted to sell cattle that was secured collateral for his farm loan, without permission from USDA/FSA. Whitacre provided agents a photo of a female in lingerie with what appeared to be gold bars in the background. Whitacre advised that this photo was of "Felicia Jackson."

17. On March 2, 2020, USDA/OIG Special Agents visited the Farmer's Livestock Exchange in Winchester, VA and obtained cattle sales records associated with WHITACRE. A

review of the records revealed that on various dates, beginning on December 2, 2019, and continuing through February 24, 2020. WHITACRE continued selling cattle that was pledged as collateral to USDA/FSA, without permission from USDA/FSA. To hide these sales from the USDA/FSA, WHITACRE sold the cattle in Wayne Robinson's name. According to the records obtained from Farmer's Livestock Exchange, Inc., WHITACRE sold 43 head of cattle, in Wayne Robinson's name, for a net amount of $20,743.82. None of these funds were paid to USDA/FSA.

18. USDA/OIG Special Agents have determined that WHITACRE sold and disposed of a total of 171 head of cattle which were secured USDA/FSA collateral, with a total net value of $91,624.17. The records and interviews indicate that, less the November 18, 2019 check for $16,910.69 which was intercepted by FSA and applied to WHITACRE's loan, WHITACRE received $74,713.48 in proceeds from the cattle sales. USDA/OIG agents believe that most, if not all, of the $74,713.48 in funds that WHITACRE received from the cattle sales was sent to the subject(s) in California.

GOOGLE

19. Through my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access, to the general public. Google allows subscribers to obtain email accounts at the domain name Google, like the email account listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. The computers of Google are likely to contain stored electronic communications (including retrieved and un-retrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account

application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

20. In general, an email that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google servers indefinitely.

21. Emails stored in a subscriber's mail box may contain information pertaining to new social media and/or cellular phone application accounts that were created such as emails stored in a subscriber's mail box may contain account activation emails that require verification to create new social media and/or cellular phone application accounts. Such account activation emails can indicate that the subscriber of the email account received notification and/or verified the creation of new social media and cellular phone application accounts. This is particularly important if such new social media and/or cellular phone application accounts were used to conduct illicit activities, such as contacting victims.

22. When the subscriber sends an email, it is initiated at the user's electronic device, transferred via the Internet to Google's servers, and then transmitted to its end destination. Google often saves a copy of the email sent. Unless the sender of the email specifically deletes the email from the Google server, the email can remain on the system indefinitely.

23. Subscribers to Google might not store on their home computers copies of the emails stored in their Google account. This is particularly true when they access their Google account through the web, or if they do not wish to maintain particular emails or files in their residence. A Google subscriber can also store files, including emails, address books, contact or buddy lists,

pictures, and other files, on servers maintained and/or owned by Google including updating many functions, applications, and drives on Google's cloud storage system, Google Drive.

24. Google Drive is a cloud storage and synchronization service developed by Google. Google Drive allows users to store files on its servers, synchronize files across devices, and share files. In addition to a website, Google Drive offers apps with offline capabilities for Windows and macOS computers as wells as Android and iOS smartphones and tablets. A person may sign up for Google Drive, Gmail, Google Photos, and other Google services by creating a Google account, which provides the account user with 15 gigabytes of free cloud storage. The Google Photos app automatically sends photos to Google Drive. The Google Photos app can also automatically delete photos on your phone that have already been uploaded to Google Drive. A Gmail user is able to store email attachments sent through Gmail directly to their Google Drive. In my training and experience I am aware people may save photographs received in email attachments to their cloud storage such as Google Drive. This information may provide clues to the subscriber's identity, location, or illicit activities.

25. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

26. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contact lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). This geographic information may tend to either inculpate or exculpate the account owner. Last, stored electronic data may provide relevant insight into the email account user's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the user's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

27. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, cloud services (Google Drive) and attachments to e-mails, including pictures and files.

CONCLUSION

28. Based on the forgoing, I believe there is probable cause to search the Google account feliciajackson0247@gmail.com for emails and other information to assist law enforcement in identifying who may be using this account and where they are located, where the

misappropriated funds may now be located, and whether there are any other victims to this romance scam, among other evidence. I request that the Court issue the proposed search warrant.

29. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google, LLC. Because the warrant will be served on Google, which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

30. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

OATH

The information in this affidavit is true to the best of my knowledge and belief.

Respectfully submitted,

s/Brian McCarthy
Special Agent - USDA/OIG

Received by reliable electronic means and sworn and attested to by telephone on this 21st day of August 2020.

Joel C. Hoppe

JOEL C. HOPPE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with feliciajackson0247@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google, LLC., a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google, LLC. ("Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for the account or identifier listed in Attachment A:

a. All records and information associated with the account listed in Attachment A for the following as applicable: Gmail, Web History, Google Search History, Location History, Google Photos, Google Docs, Google Calendar, Google Maps, and Google Drive;

b. All Internet search requests inputted by the subscriber for the account listed in Attachment A and URLs and/or IP addresses typed into the web browser's address bar or URLs and/or IP addresses clicked on for the account listed in Attachment A;

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, deleted emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

d. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates,

account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

e. The types of service utilized;

f. All records or other information stored by an individual using the account, including address books, contact and buddy lists, Google Calendar, Google Wallet/Finance, pictures to include exif data, and any other files;

g. All records pertaining to devices from which the account accessed and Google services or which any Google service is synced, to include device serial numbers, model type/number, IMEI, and MAC address;

h. Information regarding network identifiers from which any Google service was accessed, to include IP addresses and associated date and time of access; and

i. All stored communications or files including the Gmail account and contents of Google Drive accounts including backup of applications and accounts; and

j. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of **18 U.S.C. § 1343**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Communications to and from David WHITACRE.

(b) Communications to and from any person or company seeking funds or indicative of a romance scam.

(c) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the Google account owner;

(d) Evidence indicating the Google account owner's state of mind as it relates to the crime under investigation;

(e) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communication, other records and information disclosed pursuant to this warrant in order to located evidence, fruits, and instrumentalities described in the warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, USDA/OIG may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.